Universidad Nacional
de San Luis

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# Taller de Defensa Cibernética

## Presentación general

Detección de ataques a componentes de la Infraestructura Crítica de Ecuador, identificación de los Servidores de Comando y Control del ataque, neutralización de dichos Servidores de Comando y Control, presentación de evidencia forense ante las Naciones Unidas de haber sido objeto de una Ciber Agresión

# Situación inicial

- Ingenieros ecuatorianos con gran experiencia en la industria del petróleo detectaron, hace unas semanas, que los valores desplegados por tableros de control de Controladores Lógico Programables - PLC (Programmable Logic Controller) recientemente instalados, no se correspondían con la realidad de lo que estaba ocurriendo en algunos componentes de la infraestructura crítica de la industria petrolera de Ecuador.

- Días antes habían ocurrido incidentes análogos en el ámbito de sistemas SCADA - Supervisory Control And Data Acquisition, en este caso pertenecientes a instalaciones de distribución de energía eléctrica.

- Profesionales de muy alto nivel, pertenecientes a la Unión Internacional de Telecomunicaciones, integrando eficaces equipos con expertos de Ecuador, determinaron que se trató de un Ciber Ataque mediante la utilización de un Ciber Arma de arquitectura similar a Stuxnet pero con sistemas de guiado muy mejorados respecto de la versión utilizada en Natanz (Irán)

- Luego de un detallado control se re habilitaron al uso los citados elementos de la infraestructura crítica de Ecuador

# Acciones en lo inmediato



- A partir de un asesoramiento del Ministerio de Defensa, el Poder Ejecutivo de Ecuador determinó:
  - Utilizar sistemas del tipo honeypot en el ámbito de los elementos más sensitivos de la infraestructura crítica de Ecuador
  - Definir dichos elementos de alta sensibilidad
  - Definir cuántos sistemas honeypot se asignarán a cada uno de dichos elementos más sensitivos y la función de los honeypot en cada caso
  - Adquirir capacidades de alerta y detección temprana (incluyendo la capacidad de identificación de los Servidores de Comando y Control de Ciber Ataques)
  - Adquirir capacidades para ejercer los derechos derivados del Artículo 51 de la Carta de las Naciones Unidas
    - Capacidades en lo que hace a …
    - Capacidades en el ámbito de …
    - Capacidades relacionadas con …
    - Capacidades en el ámbito de la Ciencia Forense tales que …..

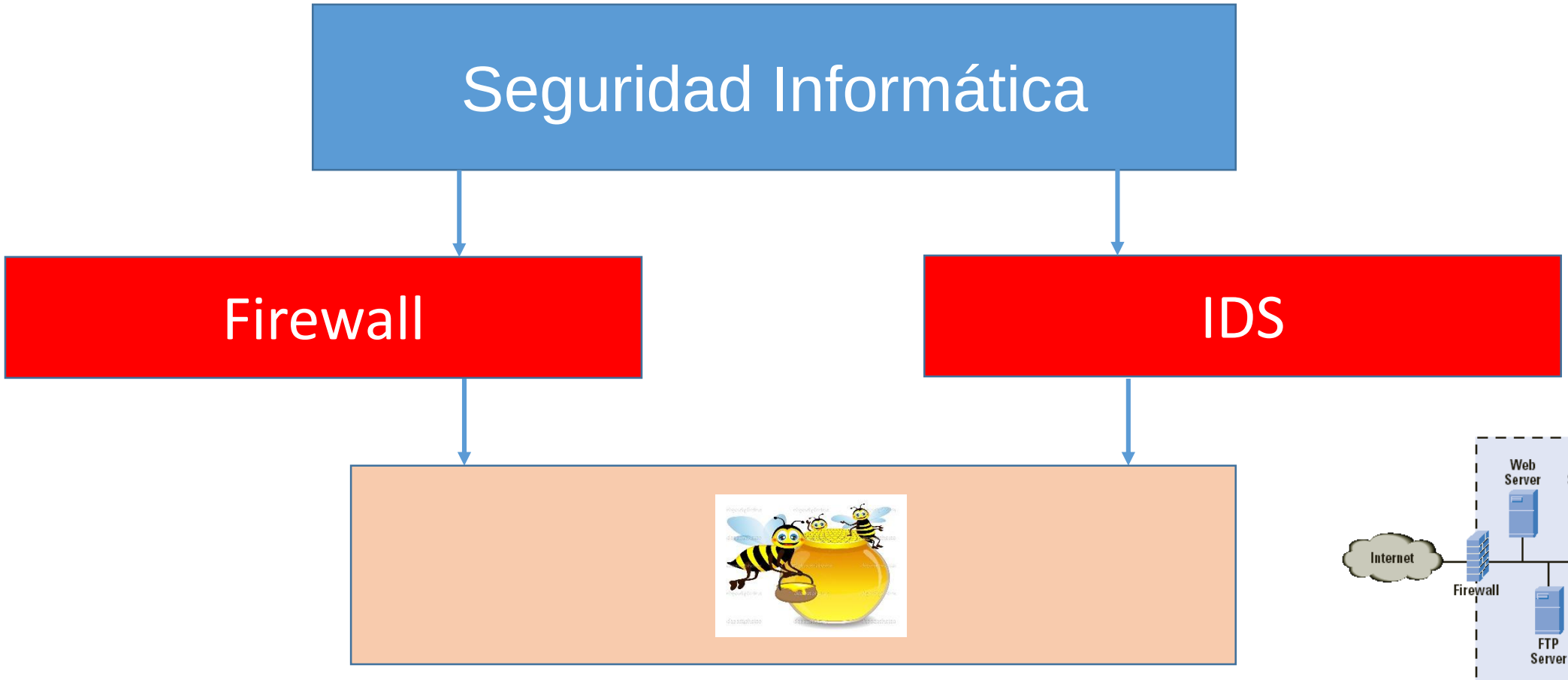
# La esencia del Taller

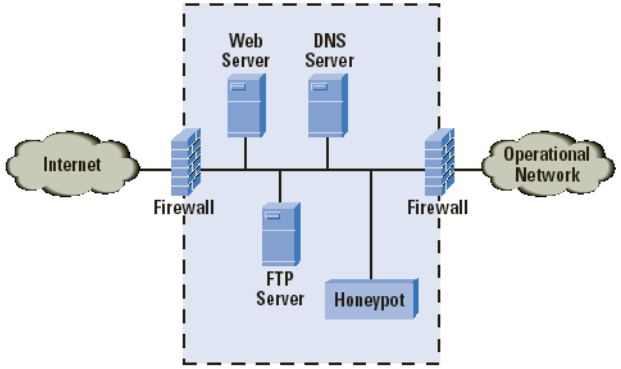
- La esencia del Taller consistirá en elaborar propuestas respecto de los cinco puntos anteriores. Dichas propuestas surgirán de grupos de discusión conformados por los asistentes aplicarán. En dichas propuestas se llevarán a términos instrumentales los contenidos desarrollados en el Seminario "Defensa Cibernética: Desafíos y oportunidades para las Fuerzas Armadas en Sudamérica"
- Las propuestas / asesoramiento consistirá en un documento breve pero de gran utilidad para las autoridades políticas y militares de Ecuador.
- El primer borrador estará listo en una hora y media a partir de esta presentación del Taller (así lo reclaman autoridades políticas del Área Defensa)

# Honeypots

- Sistemas de hardware / software destinados a atraer la atención del atacante manifestando una verosimilitud tal que haga que el atacante lo confunda con el blanco real.
- Finalidades de distintos tipos de honeypots:
  - Preservar físicamente al sistema real. Provocar que el honeypot sea el destruido en lugar sistema preservado. En algunos casos el honeypot es un “espejamiento” del sistema real conteniendo datos falsos.
  - Suministrar información falsa en operaciones de contrainteligencia.
  - Detectar tempranamente operaciones de detección de vulnerabilidades suministrando los datos iniciales que finalicen con la resolución de “Problema de la Atribución”
  - Simular la existencia de sistemas de información inexistentes en la realidad, también con un enfoque de contrainteligencia. Se los denomina honeypots de baja interacción.
  - Simular la existencia de sistemas de información desempeñándose realmente como evaluadores del poder ofensivo del adversario.
  - Ganar tiempo entre la detección del ataque y el momento en que dicho ataque llegue al núcleo del sistema protegido (el verdadero blanco). Normalmente, en este caso, se trata de honeypots de muy bajo costo de desarrollo / implantación / operación
- En el ámbito policial se suelen utilizar honeypots “clientes” dedicados a detectar, reunir pruebas y facilitar la detención de, por ejemplo, traficantes de pornografía infantil.

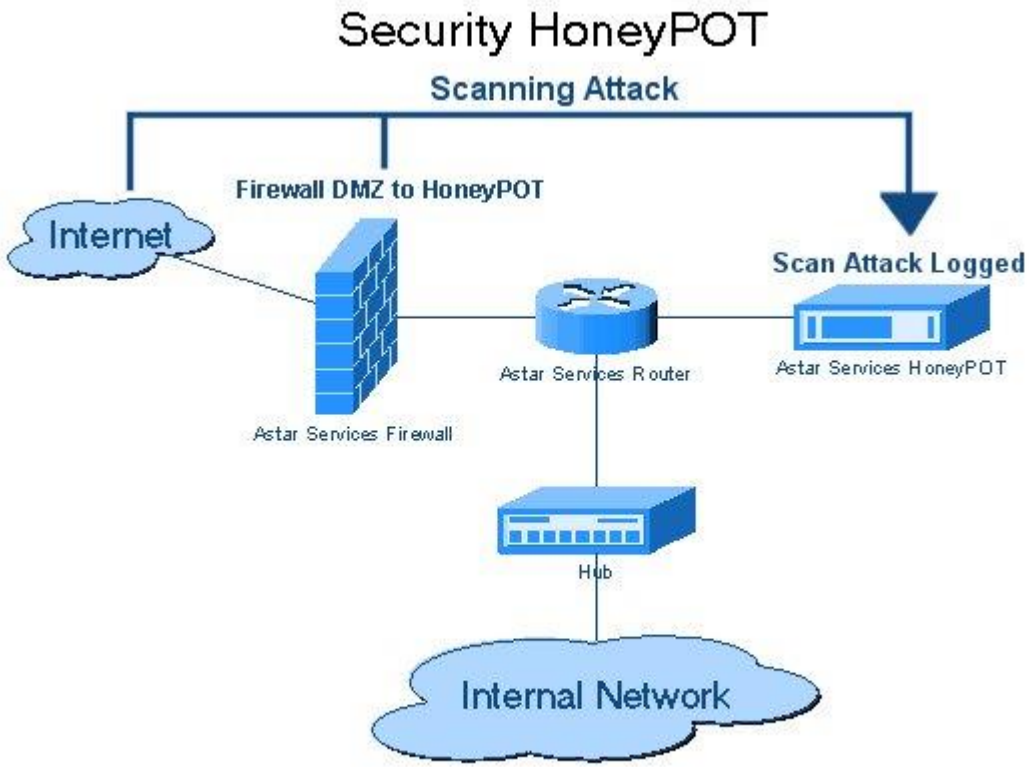
# Honeypots

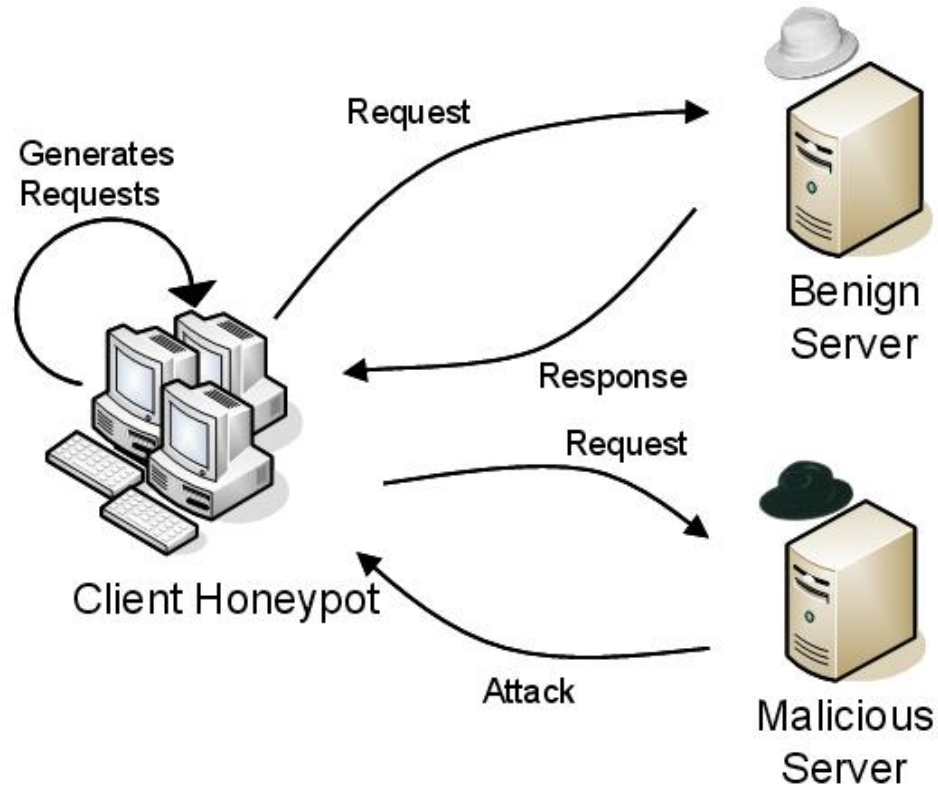


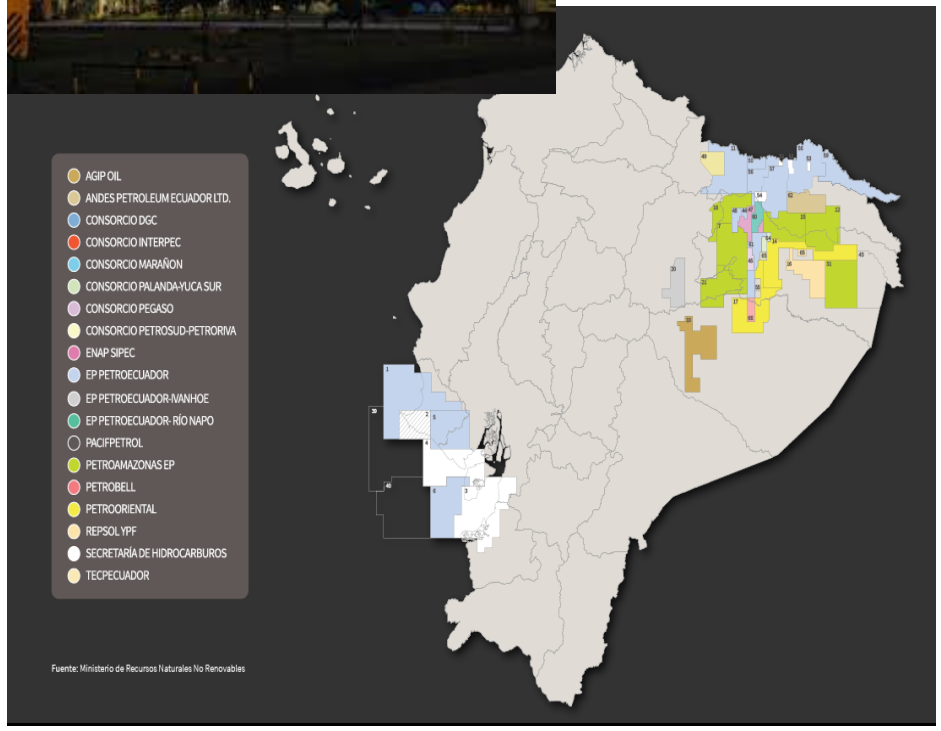

En términos conceptuales, con el honeypot, se está agregando una capa adicional de seguridad

# Honeypots


Security HoneyPOT
Scanning Attack
Firewall DMZ to HoneyPOT
Internet
Scan Attack Logged
Astar Services Router
Astar Services HoneyPOT
Astar Services Firewall
Hub
Internal Network


Request
Generates
Requests
Response
Benign
Server
Request
Client Honeypot
Attack
Malicious
Server

# Presuntos ataques

# Estructura del Informe / Asesoramiento



- Propuesta de tipo de uso de sistemas del tipo honeypot en el ámbito de los elementos más sensitivos de la infraestructura Crítica de Ecuador (definir en diez / quince líneas / renglones – asignación de tiempo: alrededor de 10/15 minutos)
- Definir las áreas / organizaciones / blancos potenciales de alta sensibilidad (respecto de Ciber Ataques) de la Infraestructura Crítica de Ecuador). Asignación de tiempo: alrededor de 10/15 minutos
- Definir cuántos sistemas honeypot se asignarán a cada uno de dichos elementos más sensitivos y la función de los honeypot en cada caso. Asignación de tiempo: alrededor de 10/15 minutos
- Adquirir capacidades de alerta y detección temprana (incluyendo la capacidad de identificación de los Servidores de Comando y Control de Ciber Ataques). Asignación de tiempo: alrededor de 10/15 minutos
- Adquirir capacidades para ejercer los derechos derivados del Artículo 51 de la Carta de las Naciones Unidas
  - Capacidades en lo que hace a …
  - Capacidades en el ámbito de …
  - Capacidades relacionadas con …
  - Capacidades en el ámbito de la Ciencia Forense tales que …..

En formato pdf, favor enviar el Informe / Asesoramiento al email del Sr. Cap. Ing. Santiago Chamorro: smchamorro@espe.edu.ec